IN THE CLAIMS

Please cancel claims 44 and 63.

With these amendments, claims 1-43, 45-62 and 64-73 remain pending.

Claims 40, 50, 52, 60, 64 and 67 have all been further amended in this response. The claims as amended are presented in the form required by Rule 121(b)(2) in the Appendix.

40. A method of decrypting data packets, comprising:

receiving a data packet from a source for a destination, the data packet including a header section and a data section, the header section storing a source identifier identifying a broadcast address of the source and a destination identifier identifying a broadcast address of the destination;

determining whether the data packet is encrypted upon reference to at least one of the source and destination identifiers; and

if the data packet is encrypted, decrypting the data packet to produce a decrypted data packet wherein the data section of the data packet includes an encrypted header section and an encrypted data section, and after decryption, the decrypted encrypted header section is used as the header for the decrypted data packet.

50. A computer program product adapted for decrypting data packets, comprising:

computer code that when executed causes the reception of a data packet from a source for a destination, the data packet including a header section and a data section, and the header section storing a source identifier identifying a broadcast address of the source and a destination identifier identifying a broadcast address of the destination;

computer code that when executed causes the determination of whether the data packet is encrypted upon reference to at least one of the source and destination identifiers;

computer code that when executed and if the data packet is encrypted, causes the decryption of the data packet to produce a decrypted data packet, wherein the data section of the data packet includes an encrypted header section and an encrypted data section, and after decryption, the decrypted encrypted header section is used as the header for the decrypted data packet; and

a computer readable medium that stores the computer codes.

52. A computer system for decrypting data packets, comprising:

a processor;

a computer readable medium coupled to the processor and storing a computer program comprising:

computer code that when executed on the processor causes the processor to receive a data packet from a source for a destination, the data packet including a header section and a data section, the header section storing a source identifier identifying a broadcast address of the source and a destination identifier identifying a broadcast address of the destination;

computer code that when executed on the processor causes the processor to determine whether the data packet is encrypted upon reference to at least one of the source and destination identifiers; and

computer code that when executed on the processor causes the processor to if the data packet is encrypted, decrypt the data packet to produce a decrypted data packet, wherein the data section of the data packet includes an encrypted header section and an encrypted data section, and after decryption, the decrypted encrypted header section is used as the header for the decrypted data packet.

60. A method of decrypting data packets, comprising:

receiving a data packet from a source at a destination, the data packet including a header section and a data section, the header section storing a source identifier, a destination identifier, and encryption information providing a mechanism for identifying an encryption method used to generate the data packet; and

decrypting the data packet to produce a decrypted data packet, wherein the data section of the data packet includes an encrypted header section and an encrypted data section, and after decryption, the decrypted encrypted header section is used as the header for the decrypted data packet.

64. A computer program product adapted for decrypting data packets, comprising:

computer code that when executed on a computer causes the computer to receive a data packet from a source at a destination, the data packet including a header section and a data

section, the header section storing a source identifier, a destination identifier and encryption information including a mechanism for identifying an encryption method used to generate the data packet;

computer code that when executed on a computer causes the computer to decrypt the data packet to produce a decrypted data packet, wherein the data section of the data packet includes an encrypted header section and an encrypted data section, and after decryption, the decrypted encrypted header section is used as the header for the decrypted data packet; and

a computer readable medium that stores the computer codes.

67. A computer system for decrypting data packets, comprising:

a processor;

a computer readable medium coupled to the processor storing a computer program comprising:

computer code that when executed on the processor causes the processor to receive a data packet from a source at a destination, the data packet including a header section and a data section, the header section storing a source identifier, a destination identifier and encryption information including a mechanism for identifying an encryption method used to generate the data packet;

computer code that when executed on the processor causes the processor to determine from the header section whether the data packet is encrypted; and

computer code that when executed on the processor causes the processor to if the data packet is encrypted, decrypt the data packet to produce a decrypted data packet, wherein the data section of the data packet includes an encrypted header section and an encrypted data section, and after decryption, the decrypted encrypted header section is used as the header for the decrypted data packet.